

THE FEDERAL BUREAU OF INVESTIGATION'S CONTROL OVER WEAPONS AND LAPTOP COMPUTERS

EXECUTIVE SUMMARY

Department of Justice (Department) components maintain a large inventory of property, such as weapons and laptop computers, that could result in danger to the public or compromise national security or investigations if not properly controlled. In March 2001, the Office of the Inspector General (OIG) audited the Immigration and Naturalization Service's (INS) management of its property and found, among other things, that the INS did not have adequate controls over weapons and computers. In particular, the audit noted that INS had categorized more than 500 weapons as lost, missing, or stolen.

After that audit, and as a result of inquiries from the Congress and the Webster Commission,¹ the Federal Bureau of Investigation (FBI) reported the loss of 445 weapons (including 351 functional weapons and 94 inoperable training weapons) and 184 laptop computers from its inventory.² In June 2001, the FBI initiated an inventory of its accountable property that, at its conclusion on March 31, 2002, revealed a total of 581 missing weapons (including 423 functional weapons and 158 inoperable training weapons) and 310 missing laptop computers.³

In response to concerns about the Department's accountability for its weapons and laptop computers, the Attorney General asked the OIG to conduct audits of the controls over the inventory of such property throughout the Department. The OIG therefore conducted separate audits of the controls over weapons and laptop computers at the FBI, the Drug Enforcement Administration (DEA), the Federal Bureau of Prisons (BOP), and

¹ The Commission for Review of FBI Security Programs, headed by former FBI Director William H. Webster.

² The FBI's report documented losses or thefts of property that occurred as long ago as April 21, 1992, for weapons and January 29, 1996, for laptop computers.

³ The FBI uses a perpetual inventory system to record the historical losses and thefts of all weapons and laptop computers. A perpetual inventory system provides a continuous record of the inventory balances, which can change daily due to inventory shrinkage or expansion resulting from losses, thefts, or the recovery of items previously reported as lost or stolen.

the United States Marshals Service (USMS).⁴ The OIG will issue separate reports on the audits of each of these components, and a capping report describing all the audits. This report covers the audit in the FBI.

As of March 2002, the FBI had an authorized strength of approximately 11,000 Special Agents and 15,000 support personnel assigned to offices throughout the United States and its territories, and in numerous foreign countries. As of August 2001, the FBI had about 50,000 weapons and 15,000 laptop computers in its property inventory.

Our audit objectives were to review the FBI's: (1) actions taken in response to the identification of lost or stolen weapons and laptop computers; and (2) management controls over these types of equipment. Although our audit focused primarily on the period from October 1, 1999 through January 31, 2002, we also reviewed losses of property outside this period to gain an understanding of the magnitude of the conditions noted in this report.⁵

The numbers of missing weapons and laptop computers reported by the FBI in July 2001 and March 2002 were taken from untested FBI data. The numbers of missing weapons and laptop computers we tested were smaller because our audit was based on items reported missing from October 1, 1999 through January 31, 2002. During that interval the FBI reported property losses of 212 functional weapons, 142 inoperable training weapons, and 317 laptop computers.⁶

Our audit revealed significant deficiencies in the FBI's management of weapons and laptop computers. The results of our audit are summarized as follows.

⁴ Since we completed an audit of the INS's management of property in March 2001, we did not include the INS in this review of weapons and laptop computers. We will, however, incorporate the results of the March 2001 audit in the capping report. We did not audit the Department's litigating components because they had very few weapons in their property inventories.

⁵ Appendix I contains additional information about our audit objectives, scope, and methodology.

⁶ These figures included losses occurring prior to October 1, 1999 but reported on or after that date. It also should be noted that, after the conclusion of our fieldwork, the FBI reported to us that it had found 8 functional weapons, 9 inoperable training weapons, and 27 laptop computers previously classified as lost or stolen.

FBI Weapons

The number of functional weapons reported missing during our review period amount to less than one-half of one percent of the FBI's current inventory of weapons. However, the significance of these losses is not measured in numbers but rather in the sensitive nature of the missing property. Whenever an agency loses weapons, there is risk of harm to the public.

Similarly, although the missing training weapons are incapable of firing live ammunition, their loss is significant because even non-functioning weapons could be used in the commission of a crime.

We identified five instances where local police recovered lost or stolen FBI weapons at crime scenes. Based on our review of the available information, we concluded that in some of those instances FBI weapons had, in fact, been used in the commission of a crime.

The FBI's response to the loss or theft of its weapons has, in our view, not been adequate. When a weapon is lost or stolen, a *Report of Lost or Stolen Property* (Form FD-500) must be submitted, but FBI policy does not give specific deadlines for submission of these forms (see Appendix XII). We reviewed the Forms FD-500 and could determine the date of submission for only 83 (39 percent) of the 212 weapons reported missing during our review period. Our review determined that most of the 83 Forms FD-500 were not submitted in a timely manner, ranging from the same day to 23 years after the loss or theft occurred. Only 7 Forms FD-500 were prepared within 5 days after a weapon became missing.

The FBI's discipline when an employee's negligence contributed to the loss or theft of weapons has been weak. We determined that only 71 of the 212 losses or thefts of functional weapons (34 percent) had been reported to the FBI's Office of Professional Responsibility (OPR).⁷ Of those 71 referrals, 31 resulted in clearing the employee in question, while another 31 resulted in disciplinary action, and 9 cases were still pending at the conclusion of our field work. The 31 disciplinary actions included 25 letters of censure, 5 suspensions ranging from 3 to 7 days in duration, and 1 six-months' probation.

⁷ Prior to 1997, field offices often handled the loss of a weapon locally, without a requirement to report the loss to the OPR.

FBI Laptop Computers

The 317 laptop computers reported missing during our review period equate to approximately 2 percent of the FBI's current inventory. Once again, however, the loss of these items is significant because of the sensitive nature of the missing property. The loss of information contained on laptop computers could compromise national security or jeopardize ongoing investigations. However, we found that until March 9, 2001, FBI policy did not even require reporting losses of laptop computers to OPR. Moreover, the FBI could not tell whether 224 of the 317 missing laptop computers (71 percent) were lost or stolen; the FBI reported merely that they could not be located.

Although we cannot be certain whether the loss of laptop computers compromised sensitive or national security information, neither can we rule out that possibility because all FBI laptop computers have access to sensitive information and are authorized for processing classified information up to the Secret level. After completing a physical inventory on March 31, 2002, the FBI reported that the security level for 70 percent of the lost or stolen laptop computers was "unknown."

As part of our audit, we reviewed the disposal of excess laptop computers and found two significant deficiencies. FBI regulations require all computers that have processed sensitive or classified information be "sanitized and declassified" before disposal. At FBI Headquarters, we tested a sample of ten laptop computers that had been excessed and found nothing in the documentation to establish whether they were free of sensitive or classified information. The FBI simply did not document that specific computers had been "sanitized and declassified."

FBI regulations also require that hard drives that processed sensitive or classified information be sent to FBI Headquarters for proper disposal. At both FBI Headquarters and the four field offices where we audited, we found nothing in the available documentation to establish whether such hard drives had been sent to FBI Headquarters for disposal. Therefore we recommend that the FBI document the completion of all required steps for disposing of excess laptop computers and hard drives that previously processed sensitive or classified information.

General Comments

We believe many of the losses of weapons and laptop computers in the FBI were avoidable. Some losses resulted from the failure of FBI employees to provide adequate safeguards for property assigned to them, and others from failure to adhere to FBI policies regarding the security of these items. To correct such deficiencies and prevent future losses, the FBI must foster an environment where all employees exercise due care for sensitive assets.

In our judgment, the FBI has not sufficiently emphasized property management. For example, the FBI did not complete a full inventory of accountable property since before 1993, despite its own policy requiring physical inventories every two years. After repeated problems with barcode technology and the loss of the primary programmer, the 1993 inventory was discontinued in 1998 when it was 84 percent complete. The 1999 inventory was discontinued in 2001 when it was 99 percent complete for field offices and 68 percent complete for Headquarters. If the FBI had completed the physical inventories of accountable property as required, we believe the FBI could have identified weaknesses in its controls and instituted timely corrective measures that might have prevented later losses.

We also found that the absence of deadlines to report the loss or theft of equipment is a serious omission from FBI policy that undermines the requirement to report losses. In our judgment, the FBI must establish and adhere to firm deadlines for reporting of every lost weapon and laptop computer, investigation of these losses and thefts by OPR, and entry of required data into the National Crime Information Center (NCIC).⁸

Department regulations require all components to submit semiannual reports to the Department Security Officer summarizing thefts of Government property that occurred within the preceding six months. We reviewed the 5 semiannual reports submitted by the FBI during our audit period and found 4 had been submitted late, with the tardiness ranging from 6 to 106 days. In addition, the semiannual theft reports were inaccurate. The overall period covered by these reports was from June 1, 1999, through November 30, 2001, during which time FBI records documented the loss or theft of 359 weapons and 152 laptop computers. However, the FBI's semiannual reports for that period reported the loss or theft of only 9 weapons and 26 laptop computers.

⁸ NCIC is a computerized index of criminal justice information, including criminal history information, fugitives, stolen property, and missing persons, available to Federal, state, and local law enforcement and other criminal justice agencies.

Deficiencies in the FBI's management of its property are not new. In 1990, the OIG reported that the FBI could not account for 2,000 pieces of ADP equipment, some of which may have contained sensitive data. Two years later the OIG found material weaknesses in some of the FBI's property acquisition and management practices. In fiscal years 1999, 2000, and 2001, the independent auditors who audited the FBI's financial statements also identified material weaknesses in the area of property management. They specifically reported the FBI needed to improve its procedures related to the timely and accurate recording, reconciliation, and reporting of property and equipment in the Property Management Application, the subsidiary record-keeping system that supports amounts reported in the annual financial statements.⁹

In this report we offer several recommendations to assist the FBI to improve its management of weapons and laptop computers. Most important, we recommend that the FBI ensure it completes future physical inventories of accountable property every two years, as its own policies require, and inventories sensitive property, including weapons and laptop computers, annually. The completion of regular inventories will give FBI managers the information they need to control assets in their custody, identify problems, and institute needed corrections.

⁹ OIG Audit Report 00-15, *Federal Bureau of Investigation Annual Financial Statement, Fiscal Year 1999*, dated July 2000, and OIG Audit Report 01-14, *Federal Bureau of Investigation Annual Financial Statement, Fiscal Year 2000*, dated May 2001. The financial statement audit report for FY 2001 has not been issued yet, but the auditors found similar weaknesses in that year as well.